INFORMATION AND COMPUTATION 85, 183–201 (1990)

Sequential Machines Realized by Group Representations

MICHAEL CONNER

The City College of New York,
140th Street and Convent Avenue, New York, New York 10031

Well-known results yield a decomposition of a sequential machine into permutation and reset machines. This paper presents a methodology for the realization of the permutation machines; this methodology involves group representation theory. In the worst case, any permutation machine can be realized by a set of matrices multiplied modulo three. Bounds on the dimensions of these matrices are given. It is further shown that realization can always be performed over roots of unity, and that appropriate fields for realization can be found by solving a very simple equation.

INTRODUCTION

Sequential machine theory is a well-established discipline in computer engineering; for small problems this theory yields specific and highly optimized designs for digital circuits. As the problems grow larger, however, the optimization algorithms usually become computationally intractable. Moreover, no one would actually write out the state table for even a modest 20 flip-flop machine since it involves over a million states.

Often one exploits some underlying structure or symmetry to simplify a large problem and arrive at a plausible if not perfectly optimized design. Starting with a general abstract sequential machine, well-known methods are used to detect various symmetries, and then some not so well known (at least in the engineering community) mathematical techniques are used to produce a highly regular, compact realization of the sequential machine (Conner and Tolimieri, 1986). The major new result given in the present paper is that computation over a finite field Z modulo p (Z_p) will always suffice for these methods. These new results yield a dramatic increase in the flexibility of the method as well as giving very tight control over the realizations.

The essence of the method is to decompose an arbitrary sequential machine into permutation-reset machines and further decompose each permutation-reset machine into a permutation machine and a reset

0890-5401/90 $3.00

machine. The semigroup of a permutation machine is a group and so has a representation over a finite dimensional vector space consisting of $N \times N$ matrices of algebraic numbers. This finite set of algebraic numbers is seen to be isomorphic to a set of elements of a finite field. The sequential machine is then realized by ordinary matrix multiplication over a finite field. Finally, it is shown that the only algebraic numbers that one need be concerned with are the various roots of unity.

First, a few motiovational theorems from sequential machine theory are stated as an introduction; many of the results from group representation theory required for the development of the method are discussed next. Several example calculations are then given to illustrate both typical and worst-case behavior of the methodology. Worst-case bounds are given. Finally, algorithms making use of the fact that only roots of unity are required are given.

Sequential Machine Theory

This section gives some definitions and results from sequential machine theory that will be useful later in the development.

Definition. A *sequential machine* is a triple $\langle S, I, \delta \rangle$ such that

S is the state set

I is the input set

$\delta: S \times I \to S$ called the next state mapping.

(A machine is *strongly connected* if any state can be reached from any other state by the application of some input sequence.)

(Since this paper is concerned exclusively with internal behavior, the usual definition of output set and output mapping is omitted. It should be noted that some authors use the term "finite automaton" or "transformation semigroup" for the structure referred to here as "sequential machine"; the latter term tends to stress interest in the concrete realization with circuitry rather than the more abstract concepts.) A useful tabular representation of a sequential machine is shown in Fig. 2, the inputs being at the top, present states at the side, and the body of the table giving the next states.

Definition. A *permutation machine* is a sequential machine in which each input permutes the state set, i.e., each state appears exactly once in each column of the table. (Each input to such a machine is called a permutation input.)

DEFINITION. A *reset machine* is a sequential machine in which each column is either the identity permutation or a single constant state.

DEFINITION. A *permutation-reset machine* is a sequential machine in which all columns are either reset inputs or permutation inputs.

DEFINITION. Let $M_1 = \langle S_1, I, \delta_1 \rangle$ and $M_2 = \langle S_2, S_1 \times I, \delta_2 \rangle$ be two sequential machines. By the *series connection* of the two machines $M = M_1 \ominus M_2$ it is meant that M_2 receives as input the input to the overall machine as well as the present state of M_1, i.e., $M = \langle S_1 \times S_2, I, \delta \rangle$, where $\delta(S_1 \times S_2, I) = \{\delta_1(S_1, I), \delta_2(S_2, S_1 \times I)\}$. This relationship is illustrated in Fig. 1.

Two well-known theorems [2–5] characterize a general sequential machine in terms of permutation machines and reset machines. (A somewhat more modern development of these ideas is given by Eilenberg, 1974, 1976, Lallement, 1979, and Pin, 1986.)

THEOREM. *If $M = \langle S, I, \delta \rangle$ is a permutation-reset machine, then M can be realized by a serial connection $M_1 \ominus M_2$, where M_1 is a permutation machine and M_2 is a reset machine.*

THEOREM. *Let M be an arbitrary sequential machine. Then there exists a serial connection of machines $M_1 \ominus M_2 \ominus \cdots \ominus M_r$ for some r which realizes M such that $M_i 1 \leqslant i \leqslant r$ is a permutation reset machine.*

An incidental result that justifies interest in permutation machines follows.

THEOREM (Hartmanis and Stearns, 1966). *Let M be a reset machine. M can be realized as a parallel connection of two state reset machines.*

(Parallel connection of machines is just a connection such that all machines receive the same input and there is no interaction among them. Two state means that the cardinality of the state set is two.) Thus, in the decomposition, the reset machines are particularly simple. Most of the

FIG. 1. Serial connection of $M_1 \ominus M_2$.

complication of dynamic behavior lies in the permutation machines. The static interconnecting logic can also get complicated.

The idea of the semigroup of a machine is quite important in this study.

DEFINITION. The *semigroup of a machine* $M = \langle S, I, \delta \rangle$ is the semigroup of mappings $a_i: S \to S$ defined by

$$(s)\, a_i = \delta(s, a_i) \qquad \text{for all} \quad s \in S.$$

(The $(s)a_i$ notation is convenient because the natural semigroup operation is concatenation.) A few minutes reflection will show that the semigroup of a permutation machine is a group (Hartmanis and Stearns, 1966).

GROUP REPRESENTATION THEORY

Mathematicians and physicists have been studying group representations for many years and there are a number of excellent sources in this area, although this has not been a traditional tool for the engineering community. The introductory material given here is from a variety of the sources given above with the proofs and most of the mathematical sophistication eliminated.

DEFINITION. Let G be a finite group having elements $g_1, g_2, ..., g_r$. A *(linear) representation* of G is a homomorphism $\sigma: G \to GL(V)$, i.e., σ takes G into the linear transformations of a vector space V such that $\sigma(g_1)\,\sigma(g_2) = \sigma(g_1 g_2)$ for all $g_1, g_2 \in G$.

DEFINITION. A representation is said to be *faithful* if the homomorphism σ above is an isomorphism.

The *dimension* N of the representation is just the dimension of the space V above; σ then takes elements of G into $N \times N$ matrices.

DEFINITION. Two elements t, $t' \in G$, a group, are *conjugate* if there exists $s \in G$ such that $t' = sts^{-1}$. This is an equivalence relation which partitions G into *orbits* (called *conjugacy classes* by some authors).

DEFINITION. A representation $\sigma: G \to GL(V)$ is *irreducible* if no subspace of V is invariant under all the operators of $\sigma(G)$.

DEFINITION. Two representations σ_1 and σ_2 are *similar* if there exists an invertible matrix T such that $\sigma_1(g) = T\sigma_2(g)T^{-1}$ for all $g \in G$. (The discus-

sion of numbers and dimensions of representations will consider similar representations to be the same for most purposes.)

THEOREM (Naimark and Stern, 1982). *The number of dissimilar irreducible representations of a group G is equal to the number of distinct orbits it possesses.*

THEOREM. *Let G of order g have h orbits and thus h irreducible representations. Then the dimensions* N_i, $1 \leqslant i \leqslant h$, *of the irreducible representations satisfy*

$$\sum_{i=1}^{h} N_i^2 = g.$$

Furthermore, $N_i \mid g$ *for all* $1 \leqslant i \leqslant h$.

These theorems yield some powerful technical tools for investigating the representations without actually computing them because every representation is a direct sum of irreducible representations.

These introductoctory ideas should aid in the understanding of some preliminary examples.

EXAMPLE 1. Consider the sequential machine M_1 shown in Fig. 2. The semigroup elements are calculated explicitly in Fig. 3. The semigroup table is given in Fig. 4. (Note that since this machine is a permutation machine, the semigroup is indeed a group and is in fact the quaternion group with a natural alphabetic identification.) There are five orbits in this group, namely,

$$O_1 = \{g_1\}, \quad O_2 = \{g_2\}, \quad O_3 = \{g_2, g_7\}, \quad O_4 = \{g_3, g_8\}, \quad O_5 = \{g_5, g_6\}.$$

Since there are five orbits, there are five irreducible representations having dimensions $N_1, \ldots, N_5$ such that

$$\sum_{i=1}^{5} N_i^2 = 8,$$

the order of the group, and $N_i \mid 8$, $1 \leqslant i \leqslant 5$. That the dimensions N_i must be positive implies that there is only one solution for the dimensions, namely, $N_1 = N_2 = N_3 = N_4 = 1$ and $N_5 = 2$. None of the one-dimensional representations is faithful and so they are not of much interest for realization. The lone two-dimensional representation is faithful. There is no single, computationally tractable, algorithm for finding representations of an arbitrary group. Instead, there are a variety of techniques for finding representations of specific kinds of groups and various special cases. Later

	0	1
a	c	e
b	d	f
c	b	h
d	a	g
e	g	b
f	h	a
g	f	c
h	e	d

FIG. 2. The machine M_1.

							0	0	0	0	1	1	1	1	0
			0	0	1	1	0	0	1	1	0	0	1	1	0
	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
a	c	e	b	h	g	b	d	f	e	d	f	c	d	f	a
b	d	f	a	g	h	a	c	e	f	c	e	d	c	e	b
c	b	h	d	f	e	d	a	g	h	a	g	b	a	g	c
d	a	g	c	e	f	c	b	h	g	b	h	a	b	h	d
e	g	b	f	c	d	f	h	a	b	h	a	g	h	a	e
f	h	a	e	d	c	e	g	b	a	g	b	h	g	b	f
g	f	c	h	a	b	h	e	d	c	e	d	f	e	d	g
h	e	d	g	b	a	g	f	c	d	f	c	e	f	c	h
	g_2	g_3	g_4	g_5	g_6		g_7	g_8							g_1

FIG. 3. Explicit calculation of semigroup elements of the inputs of M_1.

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	←i
g_1	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	
g_2	g_2	g_4	g_6	g_7	g_3	g_8	g_1	g_5	
g_3	g_3	g_5	g_4	g_8	g_7	g_2	g_6	g_1	
g_4	g_4	g_7	g_8	g_1	g_6	g_5	g_2	g_3	g_ig_j
g_5	g_5	g_8	g_2	g_6	g_4	g_1	g_3	g_7	
g_6	g_6	g_3	g_7	g_5	g_1	g_4	g_8	g_2	
g_7	g_7	g_1	g_5	g_2	g_8	g_3	g_4	g_6	
g_8	g_8	g_6	g_1	g_3	g_2	g_7	g_5	g_4	
↑ j									

FIG. 4. The semigroup for M_1.

in this paper certain quite specific representations will be prescribed. For the moment, however, it suffices to say that a two-dimensional representation σ can be found:

$$\sigma(g_1)=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \qquad \sigma(g_2)=\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix},$$

$$\sigma(g_3)=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \qquad \sigma(g_4)=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},$$

$$\sigma(g_5)=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}, \qquad \sigma(g_6)=\begin{bmatrix}0 & -i\\ -i & 0\end{bmatrix},$$

$$\sigma(g_7)=\begin{bmatrix}-i & 0\\ 0 & i\end{bmatrix}, \qquad \sigma(g_8)=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},$$

where $i^2=-1$.

The next step in the realization methodology requires a finite field, the elements of which are isomorphic to the algebraic integers appearing in the matrices above. A prime p and a mapping $\varphi\colon \{0\,1,\ -1,\ i,\ -i\}\to Z_p$ such that φ is an isomorphism between $\{0,\ 1,\ -1,\ i,\ -i\}$ and the image set (which may very well be a subset of Z_p). That there are five elements suggests Z_5. An element of Z_5 is required that satisfies $x^2+1=0 \bmod 5$. Two elements satisfy this equation, namely, 2 and 3. The mapping φ is defined by

$$\begin{aligned}\varphi\colon 0&\to 0\\ 1&\to 1\\ -1&\to 4\\ i&\to 2\\ -i&\to 3.\end{aligned}$$

The relevant matrices are

$$\sigma(g_1)=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \qquad \sigma(g_2)=\begin{bmatrix}2 & 0\\ 0 & 3\end{bmatrix},$$

$$\sigma(g_3)=\begin{bmatrix}0 & 1\\ 4 & 0\end{bmatrix}, \qquad \sigma(g_4)=\begin{bmatrix}4 & 0\\ 0 & 4\end{bmatrix},$$

$$\sigma(g_5)=\begin{bmatrix}0 & 2\\ 2 & 0\end{bmatrix}, \qquad \sigma(g_6)=\begin{bmatrix}0 & 3\\ 3 & 0\end{bmatrix},$$

$$\sigma(g_7)=\begin{bmatrix}3 & 0\\ 0 & 2\end{bmatrix}, \qquad \sigma(g_8)=\begin{bmatrix}0 & 4\\ 1 & 0\end{bmatrix}.$$

In this case, the underlying vector space Z_5^2 can be used to keep track of the state in the original machine M_1; the only matrices required are $\sigma(g_2)$ and $\sigma(g_3)$ corresponding to the original inputs of M_1. An explicit state encoding is shown in Fig. 5, where the operations are matrix multiplication

	$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 4 & 0 \end{bmatrix}$
a → $\begin{bmatrix} 3 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 2 \end{bmatrix}$
b → $\begin{bmatrix} 2 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 4 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 3 \end{bmatrix}$
c → $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 4 \end{bmatrix}$
d → $\begin{bmatrix} 4 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 3 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
e → $\begin{bmatrix} 0 \\ 2 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 0 \end{bmatrix}$
f → $\begin{bmatrix} 0 \\ 3 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 4 \end{bmatrix}$	$\begin{bmatrix} 3 \\ 0 \end{bmatrix}$
g → $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 3 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$
h → $\begin{bmatrix} 0 \\ 4 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 2 \end{bmatrix}$	$\begin{bmatrix} 4 \\ 0 \end{bmatrix}$

FIG. 5. Realization of M_1.

modulo 5. Note that in this method, the action of each input is encoded by 12 bits, while a standard encoding for M_1 would require 24.

Not every prime will work as a modulus. There is no solution to $x_2 + 1 = 0 \mod 7$. In fact, $x^2 + 1 = 0 \bmod p$ can be solved only if $p = 1 \bmod 4$ (Adams and Goldstein, 1976). Later it will be shown that not all algebraic numbers are necessary, and in fact only the roots of unity need be considered.

Next, the difficulties of this method are discussed.

The Worst Case

The outline of the method is clear. For a given permutation machine, find a faithful representation of the group generated by the inputs and then find an appropriate field of integers modulo a prime p in which to express the arithmetic. (A considerably sharper statement will be available at the end of this paper.) There are two main ways that this technique can give poor results, the numbers in the finite field can get too big, and the dimension of the vector space can get too big. The worst case is afforded by the dimension since the difficulty of calculation varies as N^2 in dimension but roughly logarithmically in number size.

The worst case in dimension is given by consideration of the symmetric group. This section gives the details of an algorithm (patterned after Naimark and Stern, 1982) to construct the representation of the symmetric group together with facts that will enable proof of a theorem about the worst case for this method.

Definition. The *group algebra* of a group G of order m is the set of all formal sums of the form

$$a = \sum_{i=1}^{m} a_i g_i,$$

where $a_i \in C$, the complex numbers, and $g_i \in G$. Alternatively, the group algebra may be thought of as a set of m-dimensional vectors whose basis set is associated with elements in the group. If $a = \sum a_i g_i$ and $b = \sum b_i g_i$ then the operations in the algebra are defined by

$$ra = \sum ra_i g_i$$

$$a + b = \sum (a_i + b_i) g_i$$

$$ab = \sum_{i,j} a_i b_j g_i g_j.$$

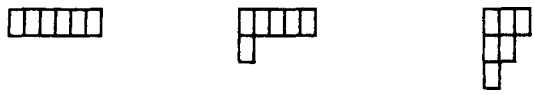

FIG. 6. Various Young's schemes for S_6.

DEFINITION. A *Young's scheme* is an arrangement of boxes such that for a given n, if there are α_i boxes in the ith row, $\alpha_1+\alpha_2+\cdots+\alpha_h=n$ and $\alpha_1\geqslant\alpha_2\geqslant\cdots\geqslant\alpha_h$, where there are h rows. Figure 6 shows various Young schemes for S_6, the symmetric group on six elements.

DEFINITION. A Young's scheme in which the integers $1, 2, ..., n$ have been placed in the boxes is called a *Young's diagram*, $\sum_\alpha$.

For a given Young's diagram $\sum_\alpha$, P_α is defined to be the set of all permutations which permute the numbers in the rows of $\sum_\alpha$ among themselves. Similarly, let Q_α be the set of all permutations which permute the elements of the columns of $\sum_\alpha$ among themselves.

DEFINITION. The *Young's symmetrizer* h_α is the element from the group algebra given by

$$h_\alpha=\sum_{p\in P_\alpha,\, q\in Q_\alpha}\sigma_q\, pq,$$

where

$$\sigma_q=\begin{cases}1 & \text{if } q \text{ is an even permutation}\\ -1 & \text{if } q \text{ is an odd permutation.}\end{cases}$$

These definitions allow easy statement of the algorithm. Let the $r=n!$ elements of the symmetric group S_n be $g_1, g_2, ..., g_r$. Choose a Young's scheme α—there will be an irreducible representation for every α—and choose a Young's diagram $\sum_\alpha$. Form P_α, Q_α, and h_α. Next form the system of elements of the group algebra $g_1h_\alpha, g_2h_\alpha, ..., g_rh_\alpha$ discarding those which are linear combinations of preceding elements. The remaining elements are written

$$a_1=g_{i_1}h_\alpha,\qquad a_2=g_{i_2}h_\alpha, ...,\qquad a_{n_\alpha}=g_{n_\alpha}h_\alpha,$$

where from the construction, $i_1=1$. These elements form a basis of the space over which the representation will act. (The proof of this fact may be found in Naimark and Stern, 1982.) Therefore, the representation of the

group element g_i, $T(g_i)$, acting on a member of the group algebra a_j is given by

$$T(g_i)a_j = \sum_{s=1}^{n_\alpha} T_{sj}(g_i)a_s.$$

This formula simply states that the action of an element of the group on a basis element must be a member of the group algebra and as such must be a linear combination of basis elements. This linear combination yields the elements of the jth row of the matrix t_{sj} that represents the group element. The action of the group element on all of the basis elements yields all of the linear combinations and hence the matrix that represents the group element. If the scheme has row lengths $\alpha_1, \alpha_2, ..., \alpha_m$, then the dimension of the representation is given by the formula (Serre, 1977)

$$n_\alpha = n! \frac{\prod_{i<j}(\tau_i - \tau_j)}{\tau_1!\,\tau_2! \cdots \tau_m!},$$

where $\tau_1 = \alpha_1 + (m-1)$, $\tau_2 = \alpha_2 + (m-2)$, ..., $\tau_m = \alpha_m$.

All representations, except for the trivial one-dimensional representations obtained from this method, are irreducible and are faithful. A simple example calculation should help clarify these ideas before statement of the main theorem of this section.

EXAMPLE 2. This example will concern the symmetric group on three elements S_3. The permutations of S_3 are shown in Fig. 7 together with an indexing scheme; the group operation is given in tabular form in Fig. 8. A Young's scheme and diagram are shown in Fig. 9. P_α is by definition the set containing two permutations: the identity permutation and the permutation that interchanges a and b, namely g_6. In the group algebra this is simply expressed as

$$P_\alpha = \{[100000], [000001]\}.$$

group elements	a	b	c ←elements to be permuted
g_1	a	b	c
g_2	c	a	b
g_3	b	c	a
g_4	a	c	b
g_5	c	b	a
g_6	b	a	c

FIG. 7. The group S_3 in tabular form.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	2	3
5	5	6	4	3	1	2
6	6	4	5	2	3	1

$\leftarrow g_i$ index

$\uparrow g_j$ index

FIG. 8. The group operation $g_i \cdot g_j$.

Similarly, Q_α is g_1 and g_5 or in the group algebra

$$Q_\alpha = \{[100000], [000010]\}.$$

The sum of all possible products (with the appropriate signs taken into account) yields the symmetrizer h_α:

$$\begin{array}{rrrrrr} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ +0 & -1 & 0 & 0 & 0 & 0 \\ \hline 1 & -1 & 0 & 0 & -1 & 1 \end{array}$$

The products of the group elements with the symmetrizer, with the appropriate linear dependencies noted, are

$$\begin{aligned} g_1 h_\alpha &= \ 1 -1 \ 0 \ 0 -1 \ 1 \\ g_2 h_\alpha &= \ 0 \ 1 -1 \ 1 \ 0 -1 \\ g_3 h_\alpha &= -1 \ 0 \ 1 -1 \ 1 \ 0 = -g_1 h_\alpha - g_2 h_\alpha \\ g_4 h_\alpha &= \ 0 \ 1 -1 \ 1 \ 0 -1 = \ g_2 h_\alpha \\ g_5 h_\alpha &= -1 \ 0 \ 1 -1 \ 1 \ 0 = -g_1 h_\alpha - g_2 h_\alpha \\ g_6 h_\alpha &= \ 1 -1 \ 0 \ 0 -1 \ 1 = \ g_1 h_\alpha . \end{aligned}$$

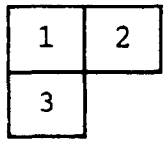

FIG. 9. A Young's diagram with scheme.

Note that since there are only two independent elements, a two-dimensional representation results as predicted by the formula above:

$$\tau_1 = 2 + (2-1) = 3$$

$$\tau_2 = 1 + (2-2) = 1$$

$$n_\alpha = 3! \frac{3-1}{3! \cdot 1!} = 2.$$

If the two basis elements chosen are $g_1 h_\alpha$ and $g_2 h_\alpha$, all that remains is to find the action of the group on the remaining basis element, $g_2 h_\alpha$, and write out the matrices explicitly:

$$g_1 g_2 h_\alpha = \quad 0 \quad 1-1 \quad 1 \quad 0-1 = \quad g_2 h_\alpha$$

$$g_2 g_2 h_\alpha = -1 \quad 0 \quad 1-1 \quad 1 \quad 0 = -g_1 h_\alpha - g_2 h_\alpha$$

$$g_3 g_2 h_\alpha = \quad 1-1 \quad 0 \quad 0-1 \quad 1 = \quad g_1 h_\alpha$$

$$g_4 g_2 h_\alpha = \quad 1-1 \quad 0 \quad 0-1 \quad 1 = \quad g_1 h_\alpha$$

$$g_5 g_2 h_\alpha = \quad 0 \quad 1-1 \quad 1 \quad 0-1 = \quad g_2 h_\alpha$$

$$g_6 g_2 h_\alpha = -1 \quad 0 \quad 1-1 \quad 1 \quad 0 = -g_1 h_\alpha - g_2 h_\alpha$$

$$T(g_1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad T(g_2) = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \quad T(g_3) = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$$

$$T(g_4) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad T(g_5) = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \quad T(g_6) = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}$$

Note that the smallest dimensional faithful representation is given by either Young's scheme shown in Fig. 10. The dimension for S_n is $n-1$ from the formula for n_α. The discussion above enables the proof of the following theorem.

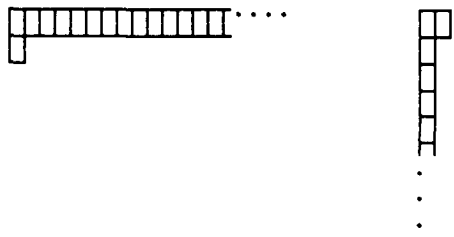

FIG. 10. Young's schemes yielding lowest dimensional representations.

THEOREM. *Any n-state permutation machine has a modular group representation realization over Z_3 having dimension $n-1$.*

Proof. Since every permutation group acting on n elements is a subgroup of S_n a representation corresponding to one of the Young schemes of Fig. 10 can be constructed having dimension $n-1$. This proof will fix on the left scheme (although either one would suffice).

The Young symmetrizer

$$h_\alpha = \sum_{P_\alpha, Q_\alpha} \sigma_q pq$$

is a sum of $2[(n-1)!]$ vectors each having $n!$ coordinates $n!-1$ of which are zero with the remaining coordinate being ± 1. No two summands are identical. This is due to the fact that Q_α contains exactly two elements, namely, the identity and the particular vertical transposition q arising from the choice of diagram $\sum_\alpha$. Therefore, the sum for h_α contains $(n-1)!$ elements that are just the horizontal permutations and $(n-1)!$ elements of the form $p_i q$, $1 \leqslant i \leqslant (n-1)!$, that are not horizontal permutations. No two elements of the sum are equal since $p_i q = p_j q$ implies $p_i = p_j$ for any group. Therefore, h_α is a vector having entries from the set $\{0, +1, -1\}$. The set $\Gamma = \{g_i h_\alpha \mid 1 \leqslant i \leqslant n!\}$ is a set of vectors having entries from the set $\{0, +1, -1\}$, since each g_i permutes the entries of h_α. There is no loss of generality in considering Γ to be a set of vectors over Z_3 the relevent partial function being $\varphi: C \to Z_3$ by

$$\varphi(0) = 0$$

$$\varphi(1) = 1$$

$$\varphi(-1) = 2.$$

The $g_i h_\alpha$ are linear combinations of $(n-1)$ basis elements, which is true in any vector space of dimension $(n-1)$. Choosing a basis and finding the linear transformations over Z_3 yields the representation. ∎

This theorem gives the worst case memory requirement for an n-state machine as growing on the order of $(n-1)^2$. This is a slightly better result than the observation that any permutation machine can be realized with permutation matrices and the underlying field does not matter as long as it has at least two elements. If one simply codes the next states in, say, binary then it is easy to see that the memory requirements can be made to vary as $n \cdot \log n$ per unit. Fortunately, rather few permutation machines require such large matrices.

When the Group Is Not the Symmetric Group

Although the case of the symmetric group gives a worst case bound of the behavior of the representation method for finding a realization of a group accumulator machine, a machine the semigroup of which is the symmetric group does not have a particularly interesting structure. That is to say, the machine can perform all possible inputs on its state set—it is a memory. Many of the more interesting sequential machines are not capable of all possible permutations. In this section, a theorem about elements from C which are required for a realization together with some observations from elementary number theory will lead to a number of interesting tools for the realization of sequential machines in the context of group representation.

DEFINITION. The *exponent* of a group G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$.

THEOREM (Curtis and Reiner, 1962). *The absolutely irreducible representations of a finite group G are all realizable in the field of nth roots of unity, where n is the exponent of G.*

THEOREM (Fermat's little theorem, Adams and Goldstein, 1976). *Let p be a prime and assume that p does not divide a. Then*

$$a^{p-1} = 1 \pmod{p}.$$

Another purely technical result, the induced representation theorem, will be required before proceeding to the main body of this section.

THEOREM (Cornwall, 1984). *Let S be a subgroup of order s of a group G of order g, and let $T_1, T_2, \ldots, T_c$ be $(c = g/s)$ coset representatives for the decomposition of G into right cosets with respect to S. Let Φ be a d-dimensional representation of S. Then the set of $cd \times cd$ matrices $\Gamma(T)$ defined for all $T \in G$ by*

$$\Gamma(T)_{kt,jr} = \begin{cases} \Phi(T_k T T_j^{-1})_{tr} & \text{if } T_k T T_j^{-1} \in S \\ 0 & \text{otherwise,} \end{cases}$$

provide a cd-dimensional representation of G.

EXAMPLE 3. This example requires a realization of the sequential machine having as its semigroup the dihedral group on seven elements. (This is the group of all rotations and reflections on a regular seven-sided

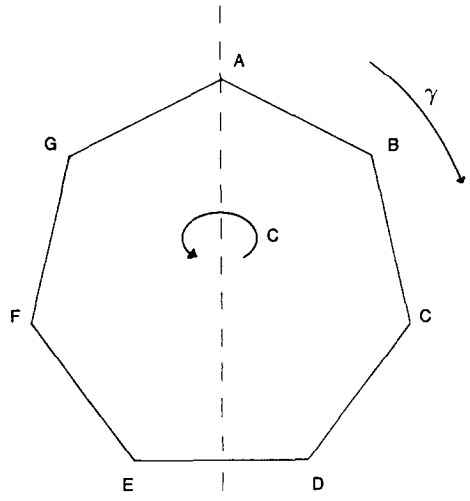

FIG. 11. Illustration of rotations and reflections of a seven-sided polygon.

polygon, as shown in Fig. 11.) A next state table which generates D_7 is shown in Fig. 12.

From the relations in D_7, $r^7 = 1$, $c^2 = 1$, and $r^i c = cr^{-i}$, where r is rotation and c is reflection, it is not difficult to determine that there are five orbits. The order of the group is 14. There is only one solution for the dimensions of the irreducible representations, namely, 1 1 2 2 2. In this example, an induced representation will be found from the subgroup of rotations. This subgroup is commutative and so it has a faithful one-dimensional representation. The exponent of D_7 is 14, so from the Curtis and Reiner theorem given above, all representations can be written by use of the 14th roots of unity. In particular, the subgroup of rotations $\{1, r, r^2, ..., r^6\}$ is represented by e^0, $e^{2\pi i/7}$, $e^{4\pi i/7}$, ..., $e^{12\pi i/7}$. To use the induced representation theorem, choose $T_1 = 1$ and $T_2 = c$ as the coset

	r	c
A	B	A
B	C	G
C	D	F
D	E	E
E	F	D
F	G	C
G	A	B

FIG. 12. Sequential machine which generates D_7.

representatives. Application of the formula given in the induced representation theorem yields

$$\Gamma(r)=\begin{bmatrix} e^{2\pi i/7} & 0 \\ 0 & e^{12\pi i/7} \end{bmatrix}, \qquad \Gamma(c)=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

This representation is over the complex numbers, in particular, the 7th roots of unity. In order to realize this machine with finite arithmetic, it is necessary to invoke Fermat's little theorem, and to do that one must solve $7n+1=p$, p a prime. The smallest n that will do is 4 and the relevant equation is $x^{28}=1 \pmod{29}$. A short trial and error process yields the fact that seven has the proper periodicity and the identifications are made yielding

$$\Gamma(r)=\begin{bmatrix} 7 & 0 \\ 0 & 25 \end{bmatrix}, \qquad \Gamma(c)=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \pmod{29}.$$

THEOREM. *Let $M=(S, I, \delta)$ be a strongly connected permutation machine. Let g be the order of G, the group accumulator of M, and let g_s be the order of the cyclic subgroup generated by some $i \in I$. Let p be the smallest prime satisfying $ng_s+1=p$ for $n \in Z$. Then M has an irreducible, faithful modular representation σ over $GF(p)$ whose dimension is g/g_s.*

Proof. That M has a linear representation over $GF(p)$ is clear from the induced representation construction and the fact that any cyclic group has a one-dimensional faithful representation. That $ng_s+1=p$, a prime, has a solution is just an instance of Dirichlet's theorem (Hardy and Wright, 1979). It remains to be shown that the induced representation is faithful and irreducible.

The induced representation technique produces a matrix which has a non-zero entry for each row and each column. The location of the non-zero entries yields the permutations between cosets. The actual numbers in $GF(ng_s+1)$ yield the subgroup structure, and, hence, the structure within the cosets.

We can think of the coset table for the group G laid out as follows:

$$\begin{array}{cccc} s_1 & s_2 & \cdots & s_{g_s} \\ c_1 & s_2c_1 & \cdots & s_{g_s}c_1 \\ \vdots & \vdots & & \vdots \\ c_{g/g_s} & & \cdots & s_{g_s}c_{g/g_s} \end{array}$$

If Γ is the induced representation and $g_1, g_2 \in G$ then

$$(\Gamma(g_1)\,\Gamma(g_2))_{kj}=\sum_w \Gamma(g_1)_{kw}\,\Gamma(g_2)_{wj};$$

but from the construction, the sum over w includes only coset representatives for which $T_k T T_j^{-1} \in S$, S being the subgroup. This implies that the sum contains only one term. Basically, the product of the two non-zero elements yields the column of the coset table while the position in the resulting vector yields the row, i.e., the coset in which the element may be found.

This representation is irreducible. Suppose that a space V' in V exists which is invariant under Γ, that is,

$$\Gamma(g)x \in V' \qquad \text{for all} \quad x \in V' \text{ and for all } g \in G.$$

This fact implies that the states represented by V'', the complement of V', cannot be reached by any input from the input set which contradicts the hypothesis of strong connectivity. ∎

CONCLUSIONS

This paper has shown that structural problems for sequential machine theory may be reduced to consideration of multiplication of matrices over finite fields. Representing matrices have been shown to exist in all cases. Further, a worst case analysis has been given in terms of the size of the matrices and the size of the finite field for the representation.

RECEIVED March 14, 1988; FINAL MANUSCRIPT RECEIVED February 23, 1989

REFERENCES

CONNER, M., AND TOLIMIERI, R. (1986), Group representation for multi-valued realization of sequential machines, *in* "Proceedings, Sixteenth international Symposium on Multiple-valued Logic, Blacksburg, VA," pp. 258–265.

KROHN, K. B., AND RHODES, J. L. (1962), Algebraic theory of machines, *in* "Proceedings, Symposium on Mathematical Theory of Automata, New York, April 25–26," Microwave Research Institute Symposium Series, Vol. XII, Polytechnic Press, Brooklyn, NY, 1963.

HARTMANIS, J., AND STEARNS, R. E. (1966), "Algebraic Structure Theory of Sequential Machines," Prentice–Hall, Englewood Cliffs, NJ, 1966.

ZEIGER, H. P., (1967), Cascade synthesis of finite-state machines, *Inform. and Control* **10**, 419–433.

BAVEL, Z. (1983), "Introduction to the Theory of Automata," Prentice–Hall, Reston, VA., 1983.

EILENBERG, S. (1974, 1976), "Automata, Languages and Machines," Vols. A, B, Academic Press, New York.

LALLEMENT, G. (1979), "Semigroups and Combinatorial Applications," Wiley, New York.

PIN, J. E. (1986), "Varieties of Formal Languages," North Oxford Academic, London; Plenum, New York.

NAIMARK, M. A., AND STERN, A. I. (1982), "Theory of Group Representations," Springer-Verlag, New York.

SERRE, J. P. (1977), "Linear Representations of Finite Groups," Springer-Verlag, New York.

BOERNER, H. (1963), "Representations of Groups," North-Holland, New York.

BURROW, M. (1965), "Representation Theory of Finite Groups," Academic Press, New York.

CORNWALL, J. F. (1984), "Group Theory in Physics," Vols. I, II, Academic Press, New York.

VAN DER WAERDEN, B. L. (1970), "Algebra," Vols. I, II, Ungar, New York.

ADAMS, W. W., AND GOLDSTEIN, L. J. (1976), "Introduction to Number Theory," Prentice-Hall, Englewood Cliffs, NJ.

CURTIS, C. W., AND REINER, I. (1962), "Representation of Finite Groups and Associative Algebras," Wiley, New York.

HARDY, G. H., AND WRIGHT, E. M. (1979), "An Introduction to the Theory of Numbers," Clarendon Press, Oxford.